Algorithms for the determination of isomorphism classes of left braces of order 64

Ramón Esteban-Romero[1]

[1]Universitat de València

The algebra of the Yang-Baxter equation
Będlewo, 11th-15th July, 2022

Aim

Main aim

- We present some ideas that could be used to determine all conjugacy subgroups of regular subgroups of the holomorph of a finite group and so all skew left braces with this additive group up to isomorphism.
- We present some partial results for left braces with additive group $C_4 \times C_4 \times C_4$.

Collaborators

New results presented here are based on joint work in progress with Adolfo Ballester-Bolinches and Vicent Pérez-Calabuig.

Funding

Grant PGC2018-095140-B-I00 funded by

The holomorph of a group

Definition

Let $(G,+)$ be a group.

- The holomorph of $(G,+)$ is

$$\begin{aligned}\mathrm{Hol}(G,+) &= [(G,+)]\mathrm{Aut}(G,+)\\ &= \{(g,\alpha) \mid g \in G, \alpha \in \mathrm{Aut}(G,+)\}\end{aligned}$$

  with the operation given by

$$(g,\alpha)(h,\beta) = (g+\alpha(h), \alpha\circ\beta).$$

- The identity element of $\mathrm{Hol}(G,+)$ is $(0,1)$.
- The subgroup $A = \{(0,\alpha) \mid \alpha \in \mathrm{Aut}(G,+)\}$ is isomorphic to $\mathrm{Aut}(G,+)$. We identify A with $\mathrm{Aut}(G,+)$.

The holomorph of a group

Definition

The group Hol$(G,+)$ acts on $(G,+)$ by means of

$$(g,\alpha) * h = g + \alpha(h), \qquad g,h \in G, \quad \alpha \in \mathrm{Aut}(G,+).$$

This action is faithful. Hence we can identify Hol$(G,+)$ with a subgroup of the group Σ_G of all permutations of G.

The holomorph of a group

A description

- Given $g \in G$, let $\tau_g \colon G \longrightarrow G$ be given by $\tau_g(h) = g + h$, $h \in G$, the left translation of G defined by g.
- It is clear that $T = \{\tau_g \mid g \in G\}$ is a subgroup of Σ_G isomorphic to G.
- Note that $\tau_g \in \Sigma_G$ acts as $(g, 1) \in \mathrm{Hol}(G, +)$.

Proposition 1

The normaliser in Σ_G of T coincides with $\mathrm{Hol}(G, +)$.

In fact, $\mathrm{Aut}(G, +)$ is the stabiliser of 0 in $\mathrm{N}_{\Sigma_G}(T)$.

Regular subgroups of Hol(G, $+$)

Characterisations

- First of all, note that a subgroup H of $\mathrm{Hol}(G,+) \leq \Sigma_G$ is regular if, and only if, it acts transitively on G and the stabiliser H_g of each $g \in G$ is trivial.
- In other words, given h, $k \in G$, there exists a unique $(g, \alpha) \in H$ such that $(g, \alpha) * k = h$.
- Suppose that H is a regular subgroup of $\mathrm{Hol}(G,+)$.
- Given $h \in G$, there exists a unique $(g, \alpha) \in H$ such that $(g, \alpha) * 0 = h$. Consequently, $g + \alpha(0) = g = h$.

Regular subgroups of Hol$(G,+)$

Characterisations

- Suppose (g,α), $(g,\beta) \in H$. Since $g = (g,\alpha) * 0 = (g,\beta) * 0$, the regularity of the action of H on G shows that $\alpha = \beta$. Hence, α is uniquely determined by $g \in G$, let us call $\alpha = \lambda_g$.
- Furthermore, since the action is transitive, the "projection" of H on the G-component of Hol$(G,+)$ is surjective.
- Consequently $H = \{(g,\lambda_g) \mid g \in G\}$, where the map $\lambda\colon G \longrightarrow G$, $\lambda(g) = \lambda_g$ depends on H.
- Note that $(0,1) * 0 = 0$, therefore $\lambda_0 = 1$ and $H \cap \mathrm{Aut}(G,+) = \{(0,1)\}$.

Regular subgroups of Hol$(G,+)$

Characterisations for the finite case

Proposition 2

Let $(G,+)$ be a finite group and let H be a subgroup of Hol$(G,+)$*. Let us denote by π_G the "projection" of $H \leq$ Hol$(G,+)$ on G. Then $|H| = |\pi_G(H)||H \cap \mathrm{Aut}(G,+)|$.*

When we compute all regular subgroups of Hol$(G,+)$, with $(G,+)$ finite, Proposition 2 is useful to discard subgroups that cannot contain regular subgroups because the "projection" to G is not surjective.

Regular subgroups of Hol$(G,+)$

Characterisations for the finite case

Proposition 3 (cf. [AB20])

Let $(G,+)$ be a finite group. Every two of the following three statements about a subgroup H of Hol$(G,+)$ *imply the other one.*

1. $|H| = |G|$.
2. $H \cap \mathrm{Aut}(G,+) = \{(0,1)\}$.
3. *The restriction to H of π_G is surjective.*

Moreover, a subgroup H of Hol$(G,+)$ *satisfying two of the three previous properties (and so the other one) is regular.*

E. Acri and M. Bonatto.
Skew braces of order p^2q I: Abelian type.
Alg. Colloq., 29(2):297–320, 2020.

Regular subgroups of Hol$(G,+)$

Properties

We have not found the next proposition in the literature.

Proposition 4

Let H be a regular subgroup of Hol$(G,+)$ *with $(G,+)$ a group and let $(g,\alpha) \in$ Hol$(G,+)$. Then $(g,\alpha)H(g,\alpha)^{-1}$ is again a regular subgroup of* Hol$(G,+)$.

Proposition 5

Suppose that $(g,\alpha) \in$ Hol$(G,+)$ and that H is a regular subgroup of Hol$(G,+)$. *Then there exists $\beta \in$ Aut$(G,+)$ such that $(g,\alpha)H(g,\alpha)^{-1} = (0,\beta)H(0,\beta)^{-1}$.*

Skew left braces and regular subgroups

Skew left braces

A skew left brace [GV17] is a triple $(B,+,\cdot)$ where B is a set, $+$ and $\cdot$ are binary operations on B such that $(B,+)$ and $(B,\cdot)$ are groups related by the property $a(b+c) = ab - a + ac$ (the sign $\cdot$ is omited and multiplications are calculated before additions). When $(B,+)$ is abelian, we often speak of a left brace.

Proposition 6

Let $(B,+,\cdot)$ be a skew left brace. Given $a \in B$, let $\lambda_a \colon B \longrightarrow B$ be the lambda map given by $\lambda_a(b) = -a + ab$. Then $H = \{(a,\lambda_a) \mid a \in B\}$ is a regular subgroup of Hol$(G,+)$.

L. Guarnieri and L. Vendramin.
Skew-braces and the Yang-Baxter equation.
Math. Comp., 86(307):2519–2534, 2017.

Skew left braces and regular subgroups

Skew left braces

Proposition 7

Given a regular subgroup H of Hol$(G, +)$*, with* $(G, +)$ *a group, then H admits a structure of skew left brace whose additive group is isomorphic to* $(G, +)$*.*

Skew left braces and regular subgroups

Skew left braces

Proposition 8

Two regular subgroups H_1 and H_2 of Hol$(G, +)$ *induce isomorphic braces if, and only if, they are conjugate by an element of* Aut$(G, +)$.

Skew left braces and regular subgroups

Skew left braces

Note that by Proposition 5, the condition of Proposition 8 can be replaced by conjugation in Hol$(G, +)$.
Regular subgroups of Hol$(G, +)$ also appear in other contexts, like Hopf-Galois structures (see, for instance, [Byo15]).

N. P. Byott.
Solubility criteria for Hopf-Galois structures.
New York J. Math., 21:883–903, 2015.

Skew left braces and regular subgroups

Skew left braces of type $C_4 \times C_4 \times C_4$

- Bardakov, Neshchadim, and Yadav introduced an algorithm to enumerate skew left braces of a given small order that is a modification of an algorithm proposed by Guarnieri and Vendramin.
- Bardakov, Neshchadim, and Yadav enumerated all left braces of order 64 except the ones with additive group isomorphic to $C_4 \times C_4 \times C_4$ (`SmallGroup(64, 55)`) and $C_2 \times C_2 \times C_4 \times C_4$ (`SmallGroup(64, 192)`).
- Known algorithms seem to have huge memory requirements to achieve this aim.

V. G. Bardakov, M. V. Neshchadim, and M. K. Yadav.
Computing skew left braces of small orders.
Int. J. Algebra Comput., 30(4):839–851, 2020.

Skew left braces and regular subgroups

Skew left braces of type $C_4 \times C_4 \times C_4$

- GAP's implementation of Hulpke's algorithm for the determination of the conjugacy classes of subgroups of a finite soluble group requires a lot of memory for saving all intermediate subgroups at a step, but only one is used at a time.
- We replace these memory requirements by saving the obtained groups to a hard disk. We modify the implementation of Hulpke's algorithm.
- We apply Proposition 2 to avoid computation of subgroups that do not lead to regular subgroups.

A. Hulpke.
Computing subgroups invariant under a set of automorphsms.
J. Symbolic Comput., 27(4):415–427, 1999.

Skew left braces and regular subgroups

Skew left braces of type $C_4 \times C_4 \times C_4$

(This is work in progress.)

To compute the skew left braces with additive group $C_4 \times C_4 \times C_4$:

- We have obtained all conjugacy classes of regular subgroups of the Sylow 2-subgroup of Hol$(C_4 \times C_4 \times C_4)$ (overall: 31 367 678 conjugacy classes of subgroups).
- Some subgroups that are not conjugate in this Sylow 2-subgroup can be conjugate in Hol$(G, +)$.

Skew left braces and regular subgroups

Skew left braces of type $C_4 \times C_4 \times C_4$

- We classify them by
  - isomorphism class,
  - isomorphism class of the corresponding action kernel and its quotient (1442 classes), and
  - conjugacy class length in Hol$(G, +)$.
- Some of these equivalence classes are small, but there are
  - 111 with more than 10 000 conjugacy classes,
  - 63 with more than 100 000 conjugacy classes,
  - 19 with more than 500 000 conjugacy classes, and
  - 4 with more than 1 000 000 conjugacy classes.

Skew left braces and regular subgroups

Skew left braces of type $C_4 \times C_4 \times C_4$

- For each of these classes, we remove conjugate subgroups.
- This requires a lot of computing time, so we are using the calculation computer cluster Lluís Vives of the Universitat de València to speed up the computations (we thank this institution for allowing us to use it).
- At the time of preparing this report, we still do not have the numbers of conjugacy classes for 19 equivalence classes. From our partial results, we know that the number of conjugacy classes lies between 1 514 769 and 5 252 101 (we do not expect it to be larger than 1 800 000).